Sicherheit fordert Innovationen

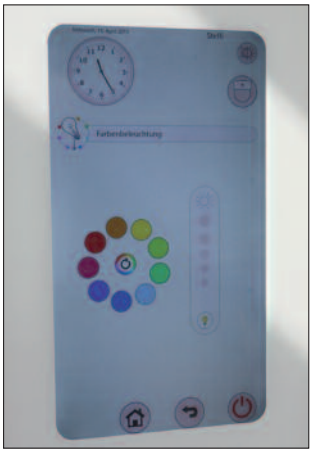
Cybercrime, IT-Sicherheit, Wirtschaftsspionage, Drohnen, Predictive Policing: „Sicherheit fordert Innovationen“ war das Thema des VfS-Kongresses am 14. und 15. April 2015 in Potsdam.

Ist unsere Sicherheitsarchitektur der aktuellen Bedrohungslage angepasst?“ Diese Frage stellte der frühere Präsident des deutschen Bundeskriminalamts, Dr. Jörg Ziercke, in seiner Keynote zur Eröffnung des Kongresses des *Verbandes für Sicherheitstechnik (VfS)*.

Als „Lackmustest“ für die Sicherheitsstrukturen bezeichnete Ziercke, wie nach den Anschlägen von Paris, Brüssel, Kopenhagen und der Absage von Veranstaltungen in Deutschland wegen befürchteter Anschläge dem Islamismus begegnet werde. Das Besondere dabei sei weniger die eigentliche Bedrohung, sondern die nicht verifizierbare Verdachtslage, etwa durch Hinweise.

Wie soll mit jenen jährlich etwa 60 bis 70 dieser Fälle umgegangen werden, die (noch) nicht zu Anschlägen geführt haben? Welche Maßnahmen sollen ergriffen werden? Schnell stehen Vorwürfe wie Panikmache oder Verunsicherung der Bevölkerung im Raum. Dazu kommt die „Strategie der 1.000 Schnitte“: Einzeltäter werden über das Internet aufgerufen, mit Messern, Pistolen und Sprengstoff Attentate zu verüben. Eine Eingrenzung der Bedrohung sei kaum möglich.

„Das Internet hat den Terror entgrenzt.“ Aus Deutschland sind etwa 650 bis 700 Kämpfer nach Syrien ausgereist. Etwa ein Drittel ist wieder zurückgekehrt, etwa 70 sind ums Leben gekommen. Im Zusammenhang mit islamistischem Terrorismus laufen in Deutschland 500 Ermittlungsverfahren. 300 Personen gelten als „Gefährder“. Weitere 300 werden als relevant für die Vorbereitung und Organisation von Anschlägen eingestuft. 40.000 Personen gelten als Sympathisanten.



VfS-Kongress: Interaktive und für Multimedia geeignete Glaswand.

Hans-Peter Stückler berichtete über Erfahrungen mit der Polizei-App Österreichs.

Die Mehrheit der Islamisten sei konservativ, apolitisch und lehne unmittelbare Gewalt ab, schaffe aber durch eine intolerante Haltung den Nährboden dafür. Klare religiöse Richtlinien geben einfache Antworten auf schwierige Fragen. Der Dschihad werde von der Avantgarde mit romantischen Vorstellungen begleitet. Menschen suchten bei den Gruppierungen eher einen emotionalen Rückhalt, ein Gefühl der Geborgenheit und Anerkennung. Es reiche nicht aus, jemandem für einen Ausstieg eine Telefonnummer zu geben, sondern es brauche einen ähnlichen Ersatz für Geborgenheit. Und das koste Geld, betonte Ziercke.

2004 wurde in Deutschland das Gemeinsame Terrorismusabwehrzentrum (GTAZ) geschaffen, als Plattform für den unmittelbaren Informationsaustausch von 40 Sicherheitsbehörden des Bundes und der Länder. Maßnahmen können rasch und effektiv umgesetzt werden.

„Im Internet schaffen Verschlüsselung und Anonymisierung einen rechtsfreien Raum, den sich die organisierte Kriminalität zu Nutze macht“, erläuterte Ziercke. „Eine zeitnahe Gefahrenabwehr wird verhindert. Wegen der schwierigen Beweislage wird die Gerechtigkeitslücke im Strafprozess immer größer.“ In Deutschland sind zwischen 550 und 600 Ermittlungsverfahren gegen 8.000 Tatverdächtige wegen organisierter Kriminalität (OK) anhängig. Der durch die OK verursachte Schaden wird auf jährlich 1,1 Milliarden Euro geschätzt. Die in Strafverfahren abgeschöpften Beträge bewegen sich demgegenüber im zweistelligen Millionen-Bereich – anders als in Italien, wo in den letzten fünf Jahren 30 Milliarden Euro abgeschöpft wurden. Der Unterschied liegt in der Umkehrung der Beweislast: Der Mafioso hat nachzuweisen, woher er das Vermögen hat, und nicht umgekehrt der Staatsanwalt ihm den unrechtmäßigen Erwerb.

Zur schweren Kriminalität zählt auch die Banden-Kriminalität, der etwa 25.000 bis 30.000 Personen zuzurechnen sind. Dazu kommen etwa 4.000 Rocker. Eine russisch-eurasische Tätergruppe („Diebe im Gesetz“) hat sich auf Wohnungseinbrüche spezialisiert. Einbrüche werden von reisenden Banden vorgenommen. „Die OK ist an der Haustüre angekommen“, sagte Ziercke. Der technische Schutz müsse verstärkt werden; es stelle sich die Frage der steuerlichen Absetzbarkeit von Einbruchsschutz.

Cybercrime. Durch die immer größer werdende Zahl von Angreifern entwickeln sich Cyberspionage und Angriffe auf den Informationsschutz zu einer Bedrohung

VfS-KONGRESS

30 Vorträge

Beim VfS-Kongress am 14. und 15. April 2015 in Potsdam wurden den etwa 260 Teilnehmern an der Tagung in drei parallelen Vortragsreihen insgesamt 30 Vorträge zu Sicherheitsthemen geboten. Unter den Referenten befand sich Dr. Hans-Peter Stückler vom Büro für Kriminalstrategie des Bundeskriminalamts. Er berichtete über Erfahrungen mit der Polizei-App Österreichs.

Der nächste VfS-Kongress wird am 5. und 6. April 2016 wiederum in Potsdam stattfinden.

www.vfs-hh.de

FOTOS: KURT HICKISCH

Jörg Ziercke: „Der Lackmustest für die Sicherheitsstrukturen ist, wie nach den Anschlägen in Europa dem Islamismus begegnet wird."

Tobias Eggendorfer: „Bei der Programmierung von Software werden die gleichen Fehler gemacht wie vor 40 Jahren."

Michael vom Hagen: „Soziale Netzwerke haben eine wichtige Rolle als Informationsquelle zum Sammeln von Informationen über Personen."

Thomas Schweer: „Der Mensch hängt an Verhaltensmustern fest, was sich auch im deliktischen Bereich zeigt."

für Unternehmen jeder Art. Als Form des Identitätsdiebstahls wurden im Frühjahr 2014 zunächst 16 Millionen und dann nochmals 18 Millionen Zugangsdaten zu Online-Shops und -Konten gestohlen. Durch gefakte Rechnungen von Telekommunikationsunternehmen wurden innerhalb von drei Wochen über 200.000 Konten kompromittiert.

Durch einen gezielten Angriff auf ein deutsches Stahlwerk über das Büronetzwerk bis in die Produktionsnetze wurden die Anlagen massiv beschädigt; Hochöfen konnten nicht mehr geregelt heruntergefahren werden. In einem anderen Fall wurde bei einem Hersteller von Steuerungsprogrammen in diese ein Schadprogramm eingeschleust, das dann mit dem Kauf der Programme „mitgekauft" wurde. Durch die hohe Leistungsfähigkeit und ständige Einsatzbereitschaft („always on") sind Smartphones mittlerweile zu idealen Teilen von Botnetzen geworden. Zudem ermöglichen sie gezielte Angriffe auf ihren Nutzer.

Die Komplexität der Informationstechnologie werde laut Ziercke durch Gebäude- und Fahrzeugsteuerung bis hin zur „digitalen Stadt" weiter zunehmen. Jedes dieser Systeme wird über das Internet angreifbar sein. Großes Angriffspotenzial bieten die von mittlerweile mehr als 100.000 Anbietern angebotenen Apps für Smartphones. Die Verantwortung für die Sicherheit der Daten wird in AGBs ausgeschlossen.

„Die Welt verändert sich durch Globalisierung, Mobilität und Technologisierung und als Abfallprodukt dieser Entwicklungen verändert sich auch die Kriminalität, die sich schnell und effektiv anpasst", betonte Ziercke. Die Struktur der Sicherheitsbehörden müsse dem gewachsen sein und mithalten können.

Forschung. In öffentlichen Räumen wie Flughäfen, Bahnhöfe, Stadien und Einkaufszentren könnte es eine Massenpanik geben. Ferner soll der Zutritt zu sicherheitskritischen Bereichen verhindert werden. An der Freien Universität Berlin wurde unter der Bezeichnung *SAFEST (Social-Area Framework for Early Security* Triggers at Airports) ein Detektionssystem entwickelt, das Einzelereignisse, wie etwa Ansammlungen von Personen, zu einem Lagebild verarbeitet. Aus der Zählung von Personen können „Dichtekarten" erstellt werden, in denen eine Häufung von Personen in verschiedenen Farben ersichtlich gemacht wrd. Das Projekt wurde sozialwissenschaftlich begleitet, um die Akzeptanz zu ermitteln.

IT-Sicherheit. „Bei der Programmierung von Software werden die gleichen Fehler gemacht wie vor 40 Jahren", sagte Prof. Dr. Tobias Eggendorfer von der Hochschule Ravensburg-Weingarten. So gebe es seit 1972 den Buffer Overflow (Überfüllen von Speicherbereichen), der bis in die heutige Zeit Schadprogrammen das Eindringen ermöglicht. Programmtechnisch wäre dies durch eine Mengenbegrenzung leicht zu verhindern. Qualitätsmanagement komme allerdings in der Softwareentwicklung nicht vor; die Kunden würden nicht danach fragen. Zusatzsoftware gegen Lücken verkaufe sich hingegen hervorragend.

Programme müssten vor der Abnahme einem Penetrations-Test unterzogen werden. In der Ausbildung zum Programmierer müssten die Folgen sicherheitsrelevanter Programmierfehler aufgezeigt und gelehrt werden.

Durch das in Deutschland geplante IT-Sicherheitsgesetz sollen kritische Infrastrukturanlagen vor Cyberangriffen geschützt, das Dunkelfeld der Sicherheitsvorfälle beleuchtet und die Zusammenarbeit zwischen Staat und Wirtschaft verbessert werden. Timo Kob *(HiSolutions AG)* wies darauf hin, dass nicht nur die Betreiber von kritischen Infrastrukturanlagen von diesem Gesetz betroffen sein werden. Erfahrungsgemäß würden die Anforderungen an nachgelagerte Unternehmen (Zulieferer) weitergeleitet.

Zum anderen werde das Gesetz Telemediendiensteanbieter verpflichten, technische und organisatorische Vorkehrungen zu treffen, die unerlaubten Zugriff verhindern und Schutz gegen äußere Angriffe bieten. Ein Telemediendienstanbieter sei aber schon jeder Betreiber einer Website, betonte Kob.

Wirtschaftsspionage. Einen Einblick in die Akteure, Mittel und Methoden der Wirtschaftsspionage bot Michael vom Hagen vom Bundesamt für Verfassungsschutz Köln. Zum Unterschied von der Konkurrenzspionage, bei der Unternehmen sich gegenseitig ausspähen, wird Wirtschaftsspionage von Staaten betrieben, um der eigenen Wirtschaft Vorteile zu verschaffen. Zum einen werden offene Quellen ausgewertet *(Offene Informationsbeschaffung – OSINT),* werden Agenten eingesetzt

Fotos: Kurt Hickisch

(Human Intelligence – HUMINT) oder Einzelpersonen („Non-Professionals“) aus dem Kreis von Gaststudenten, Praktikanten, instrumentalisiert. Eine wichtige Rolle als Informationsquelle zum Sammeln von Informationen über Personen haben auch soziale Netzwerke.

Als Vorsichtsmaßnahme sollten die wichtigsten Firmendaten (Assets; etwa Kundeninformationen, Preiskalkulation, Marktstrategie; Forschungsdaten), die erfahrungsgemäß etwa fünf Prozent der Gesamtdaten eines Unternehmens ausmachen, besonders abgesichert werden.

Hilfreich ist dabei, die Daten zu segmentieren: Nicht jeder muss auf alles Zugriff haben und nicht jeder muss alles wissen (Need-to-know-Prinzip). Internet und Intranet sind zu trennen. Wichtig ist die „Human Firewall“ – Sicherheit ist Verhalten.

Der Besucherzugang ist zu regeln, Bild- und Tonaufzeichnungen von Besuchern sind zu verbieten, Besucher sind zu begleiten. Auf Geschäftsreisen sollten Hotelzimmer nicht als sicherer Ort betrachtet werden und es sollten nur Reisedatenträger verwendet werden. Das Bundesamt für Verfassungsschutz hat eine Reihe von Broschüren herausgegeben, die heruntergeladen werden können *(www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen)*.

Drohnen. „Pro Monat werden 300.000 Drohnen an gewerbliche und private Kunden verkauft“, sagte Dr. Ingo Seebach *(Dedrone GmbH, www.dedrone.com)*. Systeme mit einer Traglast von 5 kg und einer Reichweite von 5 km sind für unter 2.000 Euro über das Internet erhältlich. Drohnen – als Multikopter im Durchmesser von 10 cm bis 2 m – können

VfS-Kongress: 50 Aussteller präsentierten ihre Produkte.

als fliegende Augen eingesetzt werden, um Industrieanlagen und öffentliche Einrichtungen auszuspionieren oder um in die Privatsphäre einzudringen. Sie können auf Nachbargebäuden positioniert und von dort als lauernde Augen oder zum Sammeln von WLAN-Daten eingesetzt werden.

Sie eignen sich, Schadfracht wie Drogen, Waffen, Sprengstoff zu transportieren, und können letztlich bewaffnet werden. Wenngleich die meisten Drohnen derzeit handgesteuert sind, kann ihr Flug auch programmgesteuert erfolgen. Pilot und Drohne müssen dann nicht miteinander verbunden sein.

Die Detektion kann optisch erfolgen, über Ultraschall, Schall, Wärmebildkameras, Frequenzmessung, und Radar. Im Fall eines Alarms gilt es, nach einer Steuerperson zu suchen und Sichtbehinderungen einzurichten.

Juristisch problematisch ist, die Funkfrequenz oder das GPS-Signal zu stören oder die Drohne physisch abzuwehren. Ein Verbot ziviler Drohnen schätzt Seebach als wenig wahrscheinlich ein. Mit hoher Wahrscheinlichkeit werden die Flugregulatorien verschärft bzw. wird, zumindest in Europa, die Installation von Transpondern als elektronischem Kennzeichen verpflichtend vorgeschrieben werden.

Predictive Policing. Der Mensch hängt an Verhaltensmustern fest, was sich auch im deliktischen Bereich zeigt. Auf eine erste Tat folgen zeitlich und örtlich zusammenhängende Straftaten („Near Repeats“) mit ähnlichen Tatmerkmalen (Deliktfeld, Beute, Modus Operandi), was etwa bei Massendelikten wie Wohnungseinbruchs- und Kfz-Diebstahl deutlich wird. Musterhaft auftretendes Verhalten lässt sich prognostizieren. Im Idealfall ist die Polizei schneller am geplanten Tatort als der Täter; Straftaten werden verhindert.

Je mehr Daten vorliegen, nicht nur mathematischer, sondern auch geografischer und sozialwissenschaftlicher Art, umso treffsicherer kann die Prognose sein.

Das von Dr. Thomas Schweer vom Institut für musterbasierte Prognosetechnik *(IfmPt; www.ifmpt.de)* vorgestellte Softwareprodukt *PRECOBS (Pre Crime Observation System)* wurde im Pilotprojekt 2002 bei der Stadtpolizei in Zürich eingesetzt und dann im Dauerbetrieb in den Kantonen Basel und Aarau.

Die Polizei in Bayern plant einen Einsatz in München und Mittelfranken. In Basel ist nach Einführung des Systems die Einbruchskriminalität um 30 Prozent gesunken. Das System wird jeden Tag aufs Neue mit Daten versorgt und errechnet, wo es zu Folgedelikten kommen könnte. Es ersetzt nicht den auswertenden Beamten, nimmt ihm aber die Analysearbeit ab. Streifentätigkeit kann gesteuert, Kapazitäten können eingespart werden.

Produkte. Beim VfS-Kongress präsentierten rund 50 Aussteller ihre Produkte. Die niederländische Firma *Recornect (www.recornect.de)* stellte eine widerstandsfähige, aber interaktive und für Multimedia geeignete Glaswand vor. Damit haben Personen, die in Verwahrung gehalten werden müssen, die Möglichkeit, sich zu beschäftigen, was Psychosen vorbeugen soll.

Es können beruhigende Raumlichter erzeugt, Bilder oder Zeichenprogramme aufgerufen werden. Über Bildtelefon kann mit Betreuern oder Familienangehörigen Kontakt aufgenommen werden. Die Funktionen werden wie bei Smartphones angetippt.

Mit dem „Detektor Avian“ von der *Sälzer GmbH (www.saelzer-security.com)* können Menschen, die sich in Fahrzeugen oder unter der Ladung verstecken, durch ihren Herzschlag entdeckt werden. Die Sensoren sind Weiterentwicklungen von seismischen Geräten und werden am Fahrgestell eines Fahrzeug angebracht, wo sie die durch den Herzschlag eines Menschen hervorgerufenen Schwingungen aufnehmen. Ein Sensor genügt. Werden vier eingesetzt, kann die Position des Versteckten angegeben werden. Aufwendige Durchsuchungen der Ladung, in der sich ein flüchtender Strafgefangener versteckt haben könnte, oder Messungen mit der CO_2-Sonde bei Verdacht auf Menschenschmuggel, können durch diese neue Technik abgelöst werden.

Kurt Hickisch

FOTO: KURT HICKISCH